Amendment of the Claims

Please amend claims 1, 22 and 44. Please cancel claims 2, 8, 18-19, 23, 37-38, 42-43 and 45-63.

1. (Currently Amended) A method for limiting the impact of undesirable behavior of computers on a network through which packets of data are interchanged between the computers, comprising:

monitoring the network for any patterns of behavior;

determining, upon discovering that one or more of the patterns of behavior is undesirable, a type of the undesirable pattern of behavior;

determining a proper action for mitigating that type of undesirable behavior, the proper action including preventing dissemination through the network of packets associated with the undesirable behavior and allowing dissemination of packets not associated with the undesirable behavior,

wherein preventing dissemination comprises at least one of changing a routing table, changing a forwarding table, turning off at least one port of a forwarding device, filtering on Internet Protocol (IP) addresses, and filtering on media access control (MAC) addresses, and

wherein a discovery, including that of a network topology, facilitates the network monitoring and type of undesirable behavior determination.

2. (Cancelled).

3. (Original) The method of claim 1, wherein the dissemination through the network of packets associated with the undesirable behavior is prevented for a time period that is lengthened gradually as long as the undesirable behavior continues or intermittently reappears, the time period being gradually shortened if the undesirable behavior stops for a predetermined time.

4. (Original) The method of claim 3, wherein the time period corresponds to a skepticism level that depends on a history of the undesirable pattern of behavior, a skepticism level zero (0) denoting a good history.

5. (Original) The method of claim 1, wherein the undesirable pattern of behavior is characterized in that it matches behavior defined by a network administrator as notable or undesirable.

6. (Original) The method of claim 1, wherein the undesirable pattern of behavior is any network pathology characterized as a broadcast storm or an address resolution protocol (ARP) fight.

7. (Original) The method of claim 1, wherein the undesirable pattern of behavior includes any one or more of a stolen Internet protocol (IP) address, a stolen media access control (MAC) address, a malformed packet, too many packets directed to an overloaded server, too many probe packets directed to a firewall or too many ARP request packets.

8. (Cancelled).

9. (Original) The method of claim 1, wherein the undesirable pattern of behavior is a broadcast storm, and wherein the monitoring includes

recovering a topology of the network using information obtained through a network management protocol interface, and

learning historical packet traffic statistics for any segment of the network.

10. (Original) The method of claim 9, wherein the network management protocol is the simple network management protocol (SNMP).

11. (Original) The method of claim 1, wherein the undesirable pattern of behavior is a broadcast storm, and wherein the monitoring includes learning a topology of the network from a forwarding database or table of a forwarding device in the network.

12. (Original) The method of the claim 1, wherein the network is a shared data network.

13. (Original) The method of claim 11, wherein the network is a switched Ethernet network and the forwarding device is a switch.

14. (Original) The method of claim 11, wherein the network is a bridged Ethernet network and the forwarding device is a bridge or a smart bridge.

15. (Original) The method of the claim 1, wherein the undesirable pattern of behavior is too many ARP requests and wherein the monitoring includes verifying stability and lack of conflicts in an IP or MAC address mapping.

16. (Previously Presented) The method of the claim 1, wherein the proper action further includes alerting a system administrator about the existence of the undesirable pattern of behavior.

17. (Original) The method of claim 1, wherein the undesirable pattern of behavior is a simultaneous use of a network address, and wherein the proper action includes disabling any address associated to the network address that contradicts an address list in a network server or disabling any associated address that is not included in a list of addresses that are allowed to map to the network address.

18. (Cancelled).

19. (Cancelled).

20. (Original) The method of claim 2, wherein understanding the network topology facilitates disablement of ports in forwarding devices that connect to offending computers.

21. (Original) The method of claim 3 wherein the time period becomes longer in a random exponential backoff before an attempt is made to allow resumption of the packets from any offending computer that originated the undesirable pattern of behavior, the time period becoming longer if the undesirable pattern of behavior reoccurs during a current backoff time, the time

period becoming shorter if the undesirable pattern of behavior disappears and does not reoccur in the current backoff time.

22. (Currently Amended) A system for limiting the impact of undesirable behavior of computers on a network through which packets of data are interchanged between the computers, comprising:

means for monitoring the packets for any patterns of behavior;

means for determining, upon discovering that one or more of the patterns of behavior is undesirable, a type of the undesirable pattern of behavior;

means for determining a proper action for mitigating that type of undesirable behavior, the proper action, performed by mitigation means, including preventing dissemination through the network of packets associated with the undesirable behavior and allowing dissemination of packets not associated with the undesirable behavior,

wherein preventing dissemination comprises at least one of changing a routing table, changing a forwarding table, and turning off at least one port of a forwarding device, and

wherein means for discovery, including that of a network topology, facilitates network monitoring and type of undesirable behavior determination.

23. (Cancelled).

24. (Previously Presented) The system of claim 22, wherein the dissemination through the network of packets associated with the undesirable behavior is prevented for a time period that is lengthened gradually as long as the undesirable behavior continues or intermittently reappears, the time period being gradually shortened if the undesirable behavior stops for a predetermined time.

25. (Previously Presented) The system of claim 24, wherein the time period corresponds to a skepticism level that depends on a history of the undesirable pattern of behavior, a skepticism level zero (0) denoting a good history.

26. (Original) The system of claim 22, wherein the undesirable pattern of behavior is characterized in that it matches behavior defined by a network administrator as notable or undesirable.

27. (Original) The system of claim 22, wherein the undesirable pattern of behavior is any network pathology characterized as a broadcast storm or an address resolution protocol (ARP) fight.

28. (Original) The system of claim 22, wherein the undesirable pattern of behavior includes any one or more of a stolen Internet protocol (IP) address, a stolen media access control (MAC) address, a malformed packet, too many packets directed to an overloaded server, too many probe packets directed to a firewall or too many ARP request packets.

29. (Original) The system of claim 22, wherein preventing the dissemination of the undesirable pattern of behavior includes discarding the packets associated with such behavior, isolating any of the computers at which such behavior originates, or isolating any network segments at which such behavior originates.

30. (Original) The system of claim 22, wherein the undesirable pattern of behavior is a broadcast storm, and wherein the monitoring means includes

means for recovering a topology of the network using information obtained through a standard SNMP (simple network management protocol) interface, and

means for learning historical packet traffic statistics for any segment of the network.

31. (Original) The system of claim 23, wherein the undesirable pattern of behavior is a broadcast storm, and wherein the monitoring means includes means for learning the topology of the network from a forwarding database or table of a forwarding device in the network.

32. (Original) The system of claim 31, wherein the network is a switched Ethernet network and the forwarding device is a switch.

33. (Original) The system of claim 22, wherein the network is a shared data network.

34. (Original) The system of claim 22, wherein the undesirable pattern of behavior is too many ARP requests and wherein the monitoring means includes means for verifying stability and lack of conflicts in an IP or MAC address mapping.

35. (Original) The system of claim 22 wherein the proper action includes alerting a system administrator about the existence of the undesirable pattern of behavior.

36. (Original) The system of claim 22, wherein the undesirable pattern of behavior is a simultaneous use of a network address, and wherein the proper action includes disabling any address associated to the network address that contradicts an address list in a network server or disabling any associated address that is not included in a list of addresses that are allowed to map to the network address.

37. (Cancelled).

38. (Cancelled).

39. (Original) The method of claim 23, wherein understanding the network topology facilitates disablement of ports in forwarding devices that connect to offending computers.

40. (Previously Presented) The system of claim 24 wherein the time period becomes longer in a random exponential backoff before an attempt is made to allow resumption of the packets from any offending computer that originated the undesirable pattern of behavior, the time period becoming longer if the undesirable pattern of behavior reoccurs during a current backoff time, the time period becoming shorter if the undesirable pattern of behavior disappears and does not reoccur in the current backoff time.

41. (Cancelled)

42. (Cancelled).

43. (Cancelled).

44. (Currently Amended) The method of claim [[42]] 22, wherein the dissemination through the network of packets associated with the undesirable behavior is prevented for a time period that is exponentially increasing as long as the undesirable behavior continues or intermittently reappears, the time period being exponentially shortened if the undesirable behavior stops for a predetermined time.

45. (Cancelled).

46. (Cancelled).

47. (Cancelled).

48. (Cancelled).

49. (Cancelled).

50. (Cancelled).

51. (Cancelled).

52. (Cancelled).

53. (Cancelled).

54. (Cancelled).

55. (Cancelled).

1 56. (Cancelled).

1 57. (Cancelled).

1 58. (Cancelled).

1 59. (Cancelled).

1 60. (Cancelled).

1 61. (Cancelled).

1 62. (Cancelled).

1 63. (Cancelled).